# NEW DESIGN OF NTRU PUBLIC KEY CRYPTOSYSTEM

**KHUSHBOO THAKUR, BIRENDRA KUMAR SHARMA, SWATI VERMA**

**Abstract**: NTRU is a fast public key cryptosystem presented in 1996 by Hoffstein,Pipher and Silverman of Brown University. It operates in the ring of polynomials $Z[X]/(X^N - 1)$,where the domain parameter N largely determines thesecurity of the system. Although N is typically chosen to be prime, Silverman proposes taking N to be a power of two to enable the use of Fast FourierTransforms. In this paper, on the basis of Hoffstein et al.'s NTRU cryptosystem, we propose a new design of NTRU public key cryptosystem based on Ring.

**Keyword:**modulo, NTRU cryptosystem, public key cryptography, polynomial.

**Introduction:** NTRU is the first public key cryptosystem not based on factorization or discrete logarithmic problem. NTRU was originally presented by Hoffstein, Pipher and Silverman in 1996 [2] and was published in [HPS] in 1998[3]. Since that time, NTRU Cryptosystem has issued a number of technical reports [6]. However, the concept of NTRU cryptosystem was already recorded in [7]. The notion of NTRU cryptosystem was introduced by Jeffrey Hoffstein and Daniel Lieman [1].NTRU is a fast public key cryptosystem that operates in the ring of truncated polynomials given by $Z[X]/(X^N - 1)$, where the domain parameter N largely determines the security of the system. Typically N is chosen to be a prime number (not for security reasons, but because having N prime maximizes the probability that the private key has an inverse with respect to a specified modulus [4]. Recently, however, Silverman has proposed taking N to be a power of two to allow the use of Fast Fourier Transforms when computing the convolution product of elements in the ring [5].

**Description of NTRU:** NTRU is based on the algebraic structure of certain polynomial rings. So it provides very fast computation to encrypt and decrypt the message. NTRU only requires$O(N^2)$ for the encrypt and decrypt the message. It has a following domain parameters (notation) which is the part of new NTRU cryptosystem

1. **q** : The large modulus to which each coefficiient is reduced.
2. **p**: The small modulus to which each coefficient is reduced.
3. **f**: A polynomial that is the private key.
4. $\mathbf{f_p}$: A polynomial in $Z[X]/(p, X^{n-1})$ (this is a private key).
5. $\mathbf{f_q}$: A polynomial in $Z[X]/(q, X^n - 1)$ (this is a private key).
6. **g:** A polynomial that is used to generate the public key h from f.
7. **h**: The public key, also a polynomial.
8. **r:** The random "blinding polynomial.
9. **m:** The plaintext message, a polynomial in $Z[X]/(p, X^n - 1)$.
10. **e**: The encrypted message, a polynomial in $Z[X]/(q, X^n - 1)$.
11. **H**: A hashing function.
12. $\mathbf{L_f}$: The set of polynomial in $Z[X]/(q, X^n - 1)$ whose coefficients satisfy $d_f$ .
13. $\mathbf{L_g}$: The set of polynomial in $Z[X]/(q, X^n - 1)$ whose coefficients satisfy $d_g$.
14. $\mathbf{L_r}$: The set of polynomial in $Z[X]/(q,X^n - 1)$ whose coefficients satisfy $d_r$.

This paper, we work in the ring $R= Z[X]/(x^n - 1)$. An element F R will be written as a polynomial or a vector,

$$F = \sum_{i=0}^{n-1} F_i x_i = [F_0, F_1 \ldots\ldots, F_{n-1}]$$

We use $\otimes$ denote multiplication in R. This otimas, multiplication is given otimas multiplication is given by by

$F \otimes G = H$ with

$H_k = \sum_{i=0}^{k} F_i G_{k-i} + \sum_{i=k+1}^{n-1} F_i G_{n+k-i} = \sum_{i+j \equiv k (modn)} F_i G_i$

$F_i G_i$ (2)

$i+j \equiv^X k(modn)$

**Organization**: The remaining parts of this paper an organized as follows. In Sec-tion 2, gives some notation and introduce a polynomial, inverse ad modulo which will we useful to our cryptosystem .In Section 3,we describe Hoffstein et al.'s NTRU public key cryptosystem . In Section 4,we proposed new desigin of NTRU public key cryptosystem based on Ring . In Section 4, we analyze the security properties of the our proposed cryptosystem. Finally, in Section 5, we give our concluding remarks.

**Brief Review of Hoffstein et al.'s NTRUpublic key cryptosystem**

- **Key Generation**- Bob choose two random polynomial f, g $\in L_g$ the polynomial f must satisfy the additional requirement that it have inverses modulo q and modulo p. We will denote these inverse by $F_q$ and $F_p$, that is,

$\mathbf{F_q \otimes f \equiv 1 \ (mod\ q)}$ and

$\mathbf{F_p \otimes f \equiv 1 \ (mod\ p)}$ $\mathbf{F_p \otimes f \equiv 1 \ (mod\ p)}$ (3)

Bob next compute the quantity

$$\mathbf{h \equiv p\, f_q^{-1} \otimes g \ (mod\ q)} \quad (4)$$

Bob's public key is the polynomial h. Bob's private key is the polynomial f although inpractice he will also want to store $F_p$.

- **Encryption**- Suppose Alice wants to send a message to Bob's. She begins by selecting a message m from the set of plaintexts $L_m$. Next she randomly choose a polynomial $\Phi \in L_\Phi$ and uses Alice's public key h to compute, $\mathbf{e \equiv p\Phi \otimes h + m \ (mod\ q)}$ (5)

This is the encrypted message which Alice transmits to Bob's.

**Decryption**- First we compute

1. $a \equiv f \otimes e$

$\equiv f \otimes p\Phi \otimes h + f \otimes m \ (mod\ q)$

$\equiv f \otimes p\Phi \otimes F_q \otimes g + f \otimes m \ (mod\ q)$

$\equiv p\Phi \otimes g + f \otimes m \ (mod\ q)$

Consider this last polynomial $p\Phi \otimes g + f \otimes m$. For appropriate parameter choices, we can ensure that all of its coefficients lie between $-q/2$ and $q/2$ , so that it doesn't change if its coefficients are reduced modulo q. This means that when Bob's reduces the coefficients of $f \otimes e$ modulo q into the interval from $-q/2$ to $q/2$, he recovers exactly the polynomial,

$\mathbf{a \equiv p\Phi \otimes g + f \otimes m \quad in Z[X]/(X^N - 1)}$

**The New design of NTRU public key cryptosystem**

The proposed cryptosystem is divided into three parts: Key generation, Encryption, and Decryption.

**Key Generation :**

- **Step 1**: To create an NTRU key, Bob's choose randomly two polynomial

$f(x) \in L_f$ and $g(x) \in L_g$ such that $F_q x$, $F_p x \in R$ satisfying,

$\mathbf{f(x) \otimes f_q(x)^{-1} = 1 \ (mod\ q)}$ and

$\mathbf{f(x) \otimes f_p(x)^{-1} = 1 \ (mod\ p).}$

- **Step 2**: Let $H(x) = p \otimes f_q(x)^{-1} \otimes g(x) \ (mod\ q)$.
- **Public Key**: H(x), p, q

**Private Key**: f(x), $f_p(x)^{-1}$

**Encryption:** To encrypt $m(x) \in L_m$ we first choose an

$r(x) \in L_r$, then compute the ciphertext:

$\mathbf{e(x) = m(x) + H(x) \otimes r(x) \ (mod\ q)}$

This is the encrypted message which Alice to Bob's.

**Decryption:** Suppose that Bob's has received the message e(x) from Alice and want to decrypt it using his private key f(x). Bob's first computes

$\mathbf{a(x) = f(x) \otimes e(x) \ (modq)}$

where he choose the coefficients of a(x) in

the interval from $-q/2$ to $q/2$. Now treating a(x) as a polynomial with integer coefficients Bob's recover the message by computing,

$\mathbf{f_p(x)^{-1} \otimes a(x) \ (modp)}$

**Security Analysis:** We analyze the security of our cryptosystem as follows. The polynomial a(X) that Bob's compute satisfies,

1. $\mathbf{a(x) = f(x) \otimes e(x) \ (mod\ q).}$

$= f(x) \otimes (m(x) + H(x) \otimes r(x))(modq).$

$=f(x) \otimes (m(x)+p \otimes f_q(x)^{-1} \otimes g(x) \otimes r(x))$ (mod q).
$=f(x) \otimes m(x)+f(x) \otimes p \otimes f_q(x)^{-1} \otimes g(x) \otimes r(x)$ (mod q).
$=f(x) \otimes m(x)+p \otimes f(x) \otimes f_q(x)^{-1} \otimes g(x) \otimes r(x)$ (mod q).
$=f(x) \otimes m(x) + pg(x) \otimes r(x)$ (mod q).

Then we choose the coefficients of a(x) in the interval from $-q/2$ to $q/2$ . By the fact that all the coefficients of $f(x) \otimes m(x) + pg(x) \otimes r(x)$ may be in the interval $-q/2$ to $q/2$ from we almost get

$\mathbf{f(x) \otimes m(x) + pg(x) \otimes r(x)}$

Then we can recover the message m by computing $m = f_p(x)^{-1} \otimes a(x)$ (mod p). The verifier of NTRU cryptosystem we now verify the polynomial b(x) is equal to the plaintext m(x).

$\mathbf{b(x) = f_p(x)^{-1} \otimes a(x)}$

$= f_p(x)^{-1} \otimes f(x) \otimes m(x)+ pg(x) \otimes r(x)$
$= f_p(x)^{-1} \otimes f(x) \otimes m(x)$(mod p) (reducing mod p, )
$= m(x)$ (mod p)

Hence b(x) and m(x) are the same modulo p.

**Conclusion:** In this paper, a new desigin of NTRU public key cryptosystem based on Ring is proposed. Anyone except the NTRU public key cryptosystem cannot generate a valid NTRU cryptosystem on a message. The NTRU cryptosystem cannot identify the association between the message and the polynomial he generated. The proposed cryptosystem satisfies the given security requirements.

**References:**

1. Hoffstein J., Lieman D., Pipher J., Silverman J.H., "NTRU": A Pub-lic key Cryptosystem, Submission to IEEE P1363 (1999). Available at http://www.manta.ieee.org/groups/1363/StudyGroup/NewFam.html.
2. Hoffstein J., Pipher J., Silverman J.H., "NTRU": A new high speed public key cryptosystem, Manuscript,August 30,1996;presentd at rump session of crypto 96.
3. Hoffstein J., Pipher J., Silverman J.H., "NTRU": A Ring Based Public KeyCryptosystem, In Proc. Of ANTS III, volume 1423 of LNCS, page,267-288.SpringerVerlag,1998.Available at http://www.ntru.com.
4. Silverman J.H., "Invertibility in Truncated Polynomial Rings", NTRU Cryp-tosystems, Technical Report No.9 (1999).Available at http://www.ntru.com.
5. Silverman J.H., "Wraps, Gaps, and Lattice Constants", NTRUCryptosystems Technical Report No.11(1999).Availableat http://www.ntru.com.
6. Silverman J.H., "Almost Inverses and Fast NTRU Key Creation", NTRU Cryptosystems Technical Report No.14,Availableathttp://www.ntru.com.

***

Research Scholar, Prof.
School of Studies in Mathematics Pt. RavishankarShukla University Raipur (C.G.)
khushboo.thakur784@gmail.com.